UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/076,441	02/19/2002	Dmitry Gryaznov	19903.0015	9854

23517 7590 11/16/2005

SWIDLER BERLIN LLP
3000 K STREET, NW
BOX IP
WASHINGTON, DC 20007

EXAMINER	
DENNISON, JERRY B	
ART UNIT	**PAPER NUMBER**
2143	

DATE MAILED: 11/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/076,441	GRYAZNOV, DMITRY	
	Examiner	Art Unit	
	J. Bret Dennison	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *8/31/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,6-8,15,20-22,29,34-36 and 58-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 6-8, 15, 20-22, 29, 34-36, and 58-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to Amendment for Application Number 10/076,441 received on 31 August 2005.

2. Claims 1, 6-8, 15, 20-22, 29, 34-36, and 58-67 are presented for examination.

3. Applicant's arguments, see Applicant's Response, filed 08/31/2005, with respect to the rejection(s) of claim(s) 1, 6-8, 15, 20-22, 29, 34-36, and 58-67 in view of the amendments made to the claims have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is provided below.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1, 15, and 29 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Applicant implies waiting a time delay. However, Examiner is unable to determine the meaning based from the specification. The closest area in which a time delay is discussed is at the top of page 12 which says "joining and leaving each channel with a suitable time delay". However, the details of waiting a time delay is unclear and it

would require undue experimentation to one of ordinary skill in the art to understand what waiting a time delay is for. Does it mean going from channel to channel? If so, Examiner has been unable to locate this in the specification.

Claim Rejections - 35 USC § 103

Claims 1, 15, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over FitzGerald, "Virus Bulletin", ISSN 0956-9979, October 1998.

5. Regarding claims 1, 15, and 29, FitzGerald disclosed a method of detecting a computer malware comprising the steps of:

joining an Internet Relay Chat server;

retrieving a list of channels of the Internet Relay Chat server;

monitoring at least one channel in the list of retrieved channels;

accepting data received from the monitored channel;

storing and logging the data received from the monitored channel (FitzGerald, page, 3, paragraphs 1 and 2 FitzGerald taught a 'bot' to monitor selected IRC channels, the bot collecting files via the DCC protocol.).

FitzGerald did not explicitly state monitoring the channels by:

joining a channel,

waiting a time delay,

leaving the channel, and

simulating user activities by transmitting a message to the channel;

However, as shown by the Free Online Dictionary of Computing; August 6, 2001; http://web.archive.org/web/20010622192251/http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?bot the definition of a bot includes any type of autonomous software that operates as an agent for a user or a program or simulates a human activity including conversing with humans or other bots within a chat room.

As shown by "Slennox's eggdrop page: what is an eggdrop?"; January 16, 2000; http://web.archive.org/web/20000116043151/http://www.egghelp.org/whatis.htm hereinafter referred to by Slennox-1, and "Slennox's eggdrop page: what is an eggdrop?"; June 17, 2001; http://web.archive.org/web/20010617224545/www.egghelp.org/commands/channels.shtml hereinafter referred to by Slennox-2, Eggdrop is an IRC bot (Slennox-1, page 1) which has the functionality of joining and leaving channels (Slennox-2, page 3).

As shown above, FitzGerald disclosed the bot collecting files via the DCC protocol, which is the Direct Client-to-Client protocol. One of ordinary skill in the art would interpret the bot to simulate being one of the clients in the direct client-to-client connection and downloading the files from the other client.

The instant specification discloses the IRC clients using the DCC protocol, accepting DCC requests (see Spec. page 15, lines 10-17).

Therefore it would have been obvious to one of ordinary skill in the art to interpret the monitoring performed by the bot of FitzGerald to include the bot simulating human activities within the channel by conversing with them, which would require the bot to join the channel, be within the channel for a certain amount of time in order to collect files

from other clients in the channel, and of course leaving the channel, as these are all well known functionalities of a bot in a channel, as shown by Slennox-1 and Slennox-2.

Claims 15 and 29 include the limitations of claim 1, requiring a system or a program product. Because FitzGerald taught a system and method for the limitations of claim 1, claims 15, and 29are rejected with the same art as being substantially similar to claim 1.

6. Regarding claims 6, 20, and 34, FitzGerald disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein the computer malware comprises at least one of a computer virus, a computer worm, or a computer Trojan horse program (FitzGerald, page 3, paragraph 3).

7. Regarding claims 7, 21, and 35, FitzGerald disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29, including analyzing the stored and logged data to detect the computer malware (FitzGerald, page 3, paragraph 2, FitzGerald disclosed that all files are scanned to detect malware).

8. Regarding claims 8, 22, 36, FitzGerald disclosed the limitations, substantially as claimed, as described in claims 7, 21, 35, including wherein the computer malware comprises at least one of a computer virus, a computer worm, or a computer Trojan horse program (FitzGerald, page 3, paragraph 3).

9. Regarding claim 58, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 1, including wherein transmitting the message to the channel is utilized for triggering the computer malware in the channel to be sent. As shown in the above rejection of claim 1, sending messages to the channel is a well-known functionality of an IRC bot, as shown by Slennox-2.

10. Regarding claim 60, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 1. FitzGerald did not explicitly state wherein an Internet Relay Chat client is utilized in the joining, the retrieving, and the monitoring. However, as explained in the rejection of claim 1, it would have been obvious for one of ordinary skill in the art at the time of the invention to incorporate the bot of FitzGerald on a client to use the DCC protocol and monitor data in the channel.

11. Regarding claim 61, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 60, including wherein the Internet Chat Relay client automatically accepts and stores the data received from the monitored channel (FitzGerald, page 3, paragraphs 1 and 2). The purpose of a bot, as shown by the definition provided above, is to operate autonomously, meaning no human interaction is required, which shows that the bot of FitzGerald automatically accepts and stores the data received from the monitored channel.

12. Regarding claim 62, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 61, including wherein the Internet Relay Chat client scans the received data to detect the computer malware (FitzGerald, page 3, paragraphs 1 and 2).

13. Regarding claim 63, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 62, including wherein the Internet Relay Chat client collects statistics (FitzGerald, page 3, paragraph 3).

14. Regarding claim 65, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 1, including wherein the received data includes direct client-to-client DCC send requests (FitzGerald, page 3, paragraph 2).

15. Regarding claim 66, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 7, including wherein the analyzing is automatically performed (FitzGerald, page 3, paragraphs 1 and 2). The purpose of a bot, as shown by the definition provided above, is to operate autonomously, meaning no human interaction is required, which shows that the bot of FitzGerald automatically analyzes the data.

16. Regarding claim 59, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 1. FitzGerald did not explicitly state wherein storing and

logging includes storing and logging receipt time of the data and a sender of the data. Examiner takes Official Notice (see MPEP § 2144.03) that "storing and logging time of receipt and the sender of data" in a computer networking environment was well known in the art at the time the invention was made. See Ji et al (U.S. Patent Number 5,889,943). (See Hughes, U.S. 6,389,472, col. 12, lines 1-15, 55-67).

17. Regarding claim 64, FitzGerald disclosed the limitations, substantially as claimed, as described in claim 63. FitzGerald did not explicitly state wherein the Internet Relay Chat client notifies an administrator of the computer malware. Examiner takes Official Notice (see MPEP § 2144.03) that "notifying an administrator of computer viruses" in a computer networking environment was well known in the art at the time the invention was made. See Spear (U.S. Patent Number 6,611,925). (See Hughes, U.S. 6,389,472, col. 12, lines 50-67).

18. The Applicant is entitled to traverse any/all official notice taken in this action according to MPEP § 2144.03, namely, "if applicant traverses such an assertion, the examiner should cite a reference in support of his or her position". However, MPEP § 2144.03 further states "See also In re Boon, 439 F.2d 724, 169 USPQ 231 (CCPA 1971) (a challenge to the taking of judicial notice must contain adequate information or argument to create on its face a reasonable doubt regarding the circumstances justifying the judicial notice)." Specifically, In re Boon, 169 USPQ 231, 234 states "as we held in Ahlert, an applicant must be given the opportunity to challenge either the

correctness of the fact asserted or the notoriety or repute of the reference cited in support of the assertion. We did not mean to imply by this statement that a bald challenge, with nothing more, would be all that was needed". Further note that 37 CFR § 1.671(c)(3) states "Judicial notice means official notice". Thus, a traversal by the Applicant that is merely "a bald challenge, with nothing more" will be given very little weight.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to J. Bret Dennison whose telephone number is (571) 272-3910. The examiner can normally be reached on M-F 8:30am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

J. B. D.
Patent Examiner
Art Unit 2143

WILLIAM C. VAUGHN, JR.
PRIMARY EXAMINER